REMARKS

The comments of the applicant below are each preceded by related comments of the examiner (in small, bold type).

3. Claims 1-2, 6-8, 9-10, 14-22, 28-34 and 41, 45, 46, 48 rejected under 35 U.S.C. 103(a) as being unpatentable over Shostack et al. (Shostack). U.S. Patent No. 6,298,445 in view of Lyle, U.S. Patent No. 6,886,102 and further in view of Shipley. U.S. Patent No. 6,119,236.

As per claim 1:

Shostack discloses a method comprising:

detecting possible security problems at client locations (6:43-46, wherein an intrusion is a possible security problem);

transmitting notice of the possible security problems across a network in real time to a home location remotely located from the locations (6:53-57, wherein sending an alarm functions as transmitting notice of the possible security problem and the system administrator resides at a home location which is the local server);

determining at the home location an anomaly based on at least the possible security problems (7:15-16, wherein the security vulnerabilities function as anomalies and the local server is the home location); and

transmitting notice of the anomaly in real time to the client locations (7:57-63; 9:10-21, wherein the software enhancement being sent is the notice of the security vulnerability, which functions as the anomaly).

Shostack fails to teach transmitting notice of the anomaly to the client location at which the possible security problem is detected. However, Lyle discloses a method wherein an event, which consists of an actual or suspected attack, is determined based on information gleaned from an internal source called a sniffer (6:52-7:18). Lyle also discloses a method wherein the responsive action, such as a message is sent to the device with the actual or suspected attack (8:21-59).

Shostack and Lyle fail to teach updating, in real time, firewalls protecting the client locations to account for the anomaly. However, Shipley discloses a method wherein a firewall is dynamically programmed, in real time, to allow for the firewall to change its response to various security breaches that occur (7:58-8:41).

As per claim 9, this is a computer readable medium version of the claimed method discussed above in claim 1 wherein all claimed limitations have also been addressed and/or cited as set forth above.

Shostack does not disclose and would not have suggested that the place of occurrence of anomaly is at client locations, as recited in amended claim 1.

Although Shostack discloses an application 44 that checks the local server for security vulnerabilities, Shostack does not disclose and would not have suggested that the application 44 determine, at the local server, an anomaly at client locations based on at least the possible security problems at the client locations. In Shostack, the application 44 checks for

vulnerabilities at the local server, whereas in claim 1, the determination made at the home location is about an anomaly at the client locations.

What is lacking in Shostack is also not disclosed and would not have been suggested by Lyle. Lyle discloses a tracking system 100 that uses a sniffer module 304 to monitor network traffic at ports of devices throughout the network (col. 7, lines 39-41). Lyle does not disclose and would not have suggested that the sniffer module 304 detect possible security problems at client locations. In FIG. 1 of Lyle, the client locations are represented as "users" connected to switches 108a and 108b. Lyle does not disclose and would not have suggested that the sniffer module 304 detects security problems at the locations of the users.

Claims 1, 9, 17, 28, and 30 are patentable for at least similar reasons as claim 1.

Claim 41

Regarding claim 41, Shostack does not disclose and would not have made obvious detecting a possible security problem at a client location, and determining, at a home location, an anomaly at the client location based on the possible security problem, as recited in amended claim 41.

Although Shostack discloses an application 44 that checks the local server for security vulnerabilities, Shostack does not disclose and would not have suggested that the application 44 determine an anomaly at the client location based on the possible security problem at the client location. The application 44 checks for vulnerabilities at the local server, whereas in claim 41, the determination made at the home location is about an anomaly at the client location.

6. Claims 42 and 52 rejected under 35 U.S.C. 103(a) as being unpatentable over Shostack (U.S. 6,298,445) in view of Lyle (U.S. 6,886,102) and further in view of Moran, U.S. Patent No. 6,826,697.

As per claim 42:

Shostack discloses a method comprising:

detecting a possible security problem at a client location (6:43-46, wherein an intrusion is a possible security problem);

transmitting notice of the possible security problem across a network in real time to a home location remotely located from the location (6:53-57, wherein sending an alarm

functions as transmitting notice of the possible security problem and the system administrator resides at a home location which is the local server);

transmitting notice of the anomaly in real time to the client location (7:57-63; 9:10-21, wherein the software enhancement being sent is the notice of the security vulnerability, which functions as the anomaly).

Shostack fails to teach determining at the home location an anomaly by at least comparing the possible security problem with information previously logged at the home location, including searching for an unexpected login. However, Lyle discloses a method wherein the event, which consists of an attack, is compared to other events that have occurred (7:50-8:11).

Shostack and Lyle fail to teach a method in which determining the anomaly comprises searching for an unexpected login. However, Moran discloses a method wherein failed login attempts are logged (19:41-20:18). A failed login attempt is an unexpected login since it is not a correct login. The login is not expecting for the login information to be wrong, therefore a failed login qualifies as an unexpected login by an unexpected user.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to combine the inventions of Shostack and Lyle with Moran because in order to make a system less vulnerable to attack as stated in Shostack (2:18-28), the ability to detect further types of attacks such as forward and backward time steps in a log file or an overflow buffer attack as stated in Moran (4:1-37) would increase the security against attacks as a whole.

Moran does not disclose and would not have suggested "searching for a successful but unexpected login," as recited in amended claim 42. What Moran discloses is logging of "failed" login attempts.

All of the dependent claims are patentable for at least the same reasons as the claims on which they depend.

Any circumstance in which the applicant has addressed certain comments of the examiner does not mean that the applicant concedes other comments of the examiner. Any circumstance in which the applicant has made arguments for the patentability of some claims does not mean that there are not other good reasons for patentability of those claims and other claims. Any circumstance in which the applicant has amended or canceled a claim does not mean that the applicant concedes any of the examiner's positions with respect to that claim or other claims.

Please apply any charges or credits to deposit account 06-1050.

Respectfully submitted,

Date: 8/1/2006

Rex Huang

Rex I. Huang
Reg. No. 57,661

Fish & Richardson P.C.
225 Franklin Street
Boston, MA 02110
Telephone: (617) 542-5070
Facsimile: (617) 542-8906

21356710.doc